Public Safety Working Group (PSWG)

23 October 2018

Laureen Kapin (US FTC)
Co-Chair

ICANN63 GAC Plenary Meeting

ICANN | GAC
Governmental Advisory Committee

ICANN

Agenda

1. Introduction and Review of PSWG Activities

2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement

3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)

Agenda

1. Introduction and Review of PSWG Activities

2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement

3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)

PSWG Activities

Strategic Goals:

1. Develop DNS Abuse and Cybercrime mitigation capabilities

2. Preserve and Improve Domain Registration Directory Service Effectiveness

3. Build Effective and Resilient PSWG Operations

4. Develop Participation in PSWG Work and Ensure Stakeholder Input

Agenda

1. Introduction and Review of PSWG Activities

2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement

3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)

WHOIS/GDPR - Impact on Law Enforcement

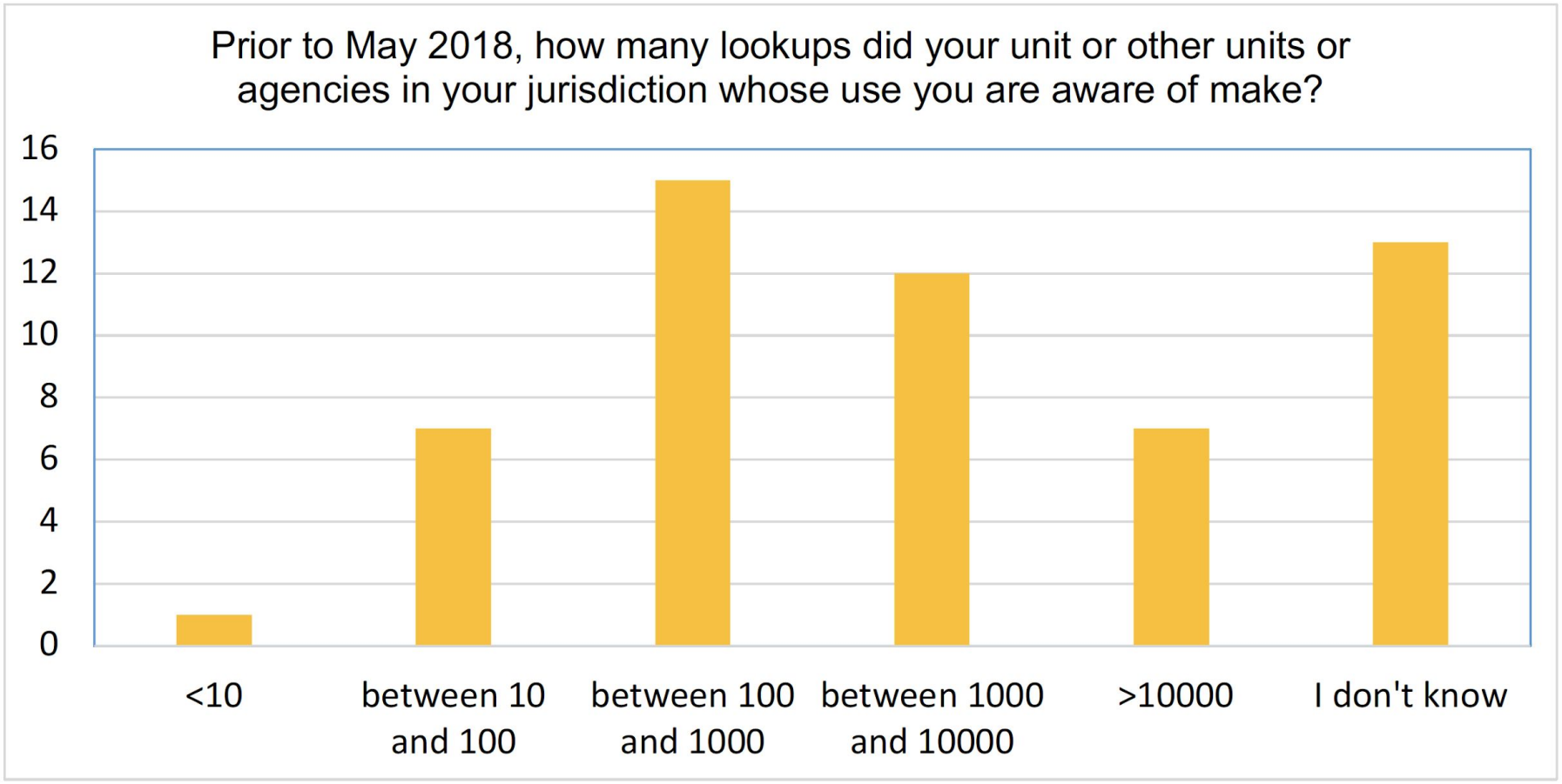
- The WHOIS/RDS2 Review Team conducted a survey of Law Enforcement agencies worldwide

- Goal:
  - to find out more about their use of the WHOIS,
  - to determine whether WHOIS met their investigative needs,
  - to provide a first assessment of the impact of changes made to the WHOIS by the Temporary Specifications adopted by the ICANN Board on 17 May 2018.

- 55 respondents (many on behalf of countries):
  Australia, Austria, Bahrain, Belgium, Brazil, Chile, China, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, India, Iran, Ireland, Italy, Japan, Kenya, Korea (South), Kuwait, Latvia, Mexico, Morocco, Nigeria, Philippines, Singapore, Slovakia, Slovenia, Sweden, Taiwan, Trinidad and Tobago, United Kingdom, United States of America and Zambia

WHOIS/GDPR - Impact on Law Enforcement

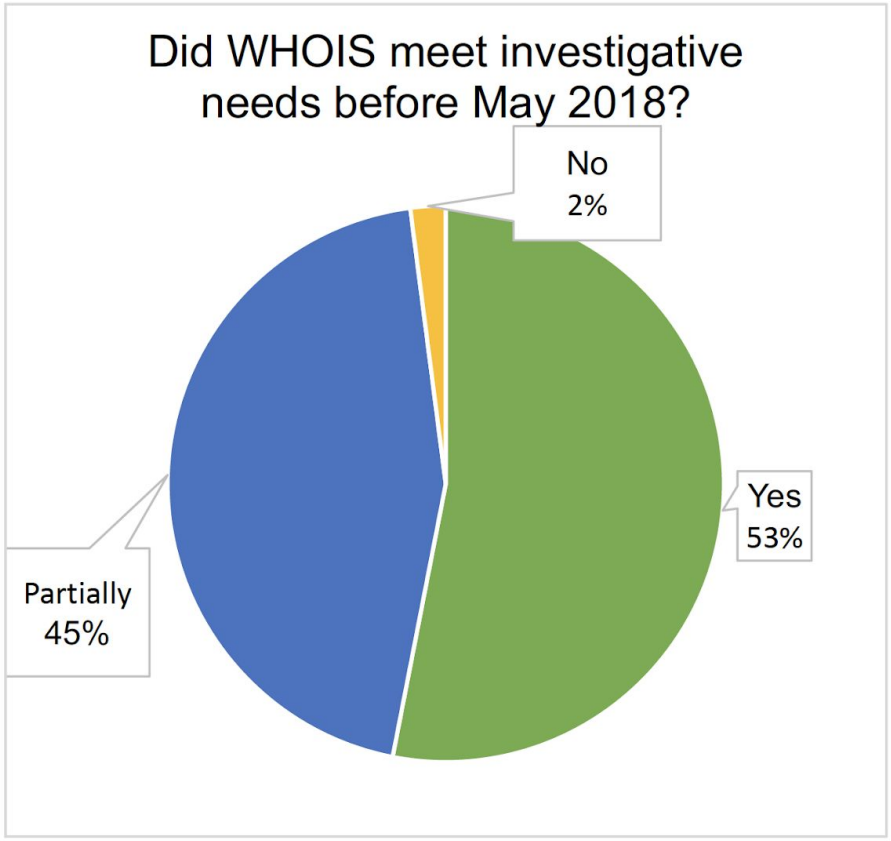
Frequency of Use

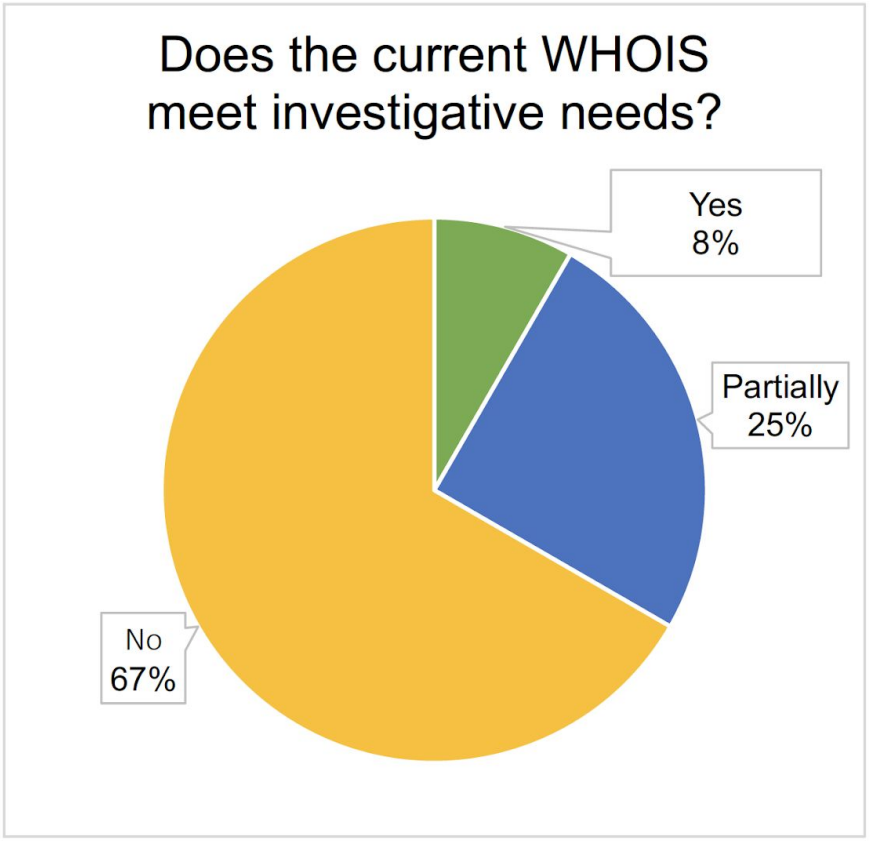


Source: WHOIS-RDS2 Review Team Initial Report Webinar, 17 September 2018

WHOIS/GDPR - Impact on Law Enforcement

Impact of Change

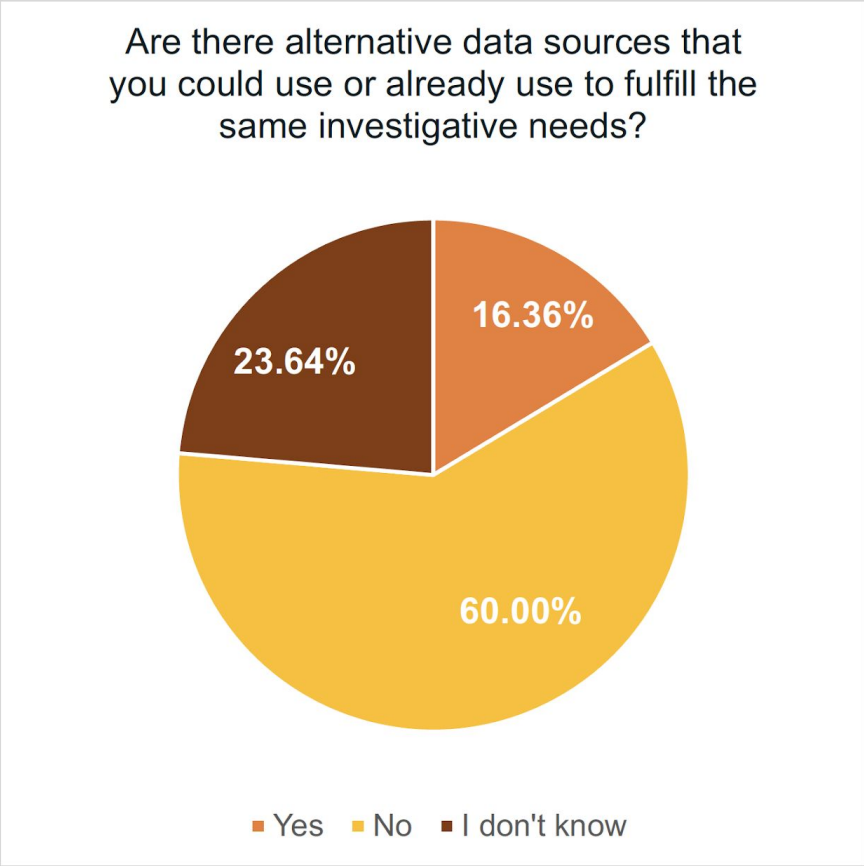


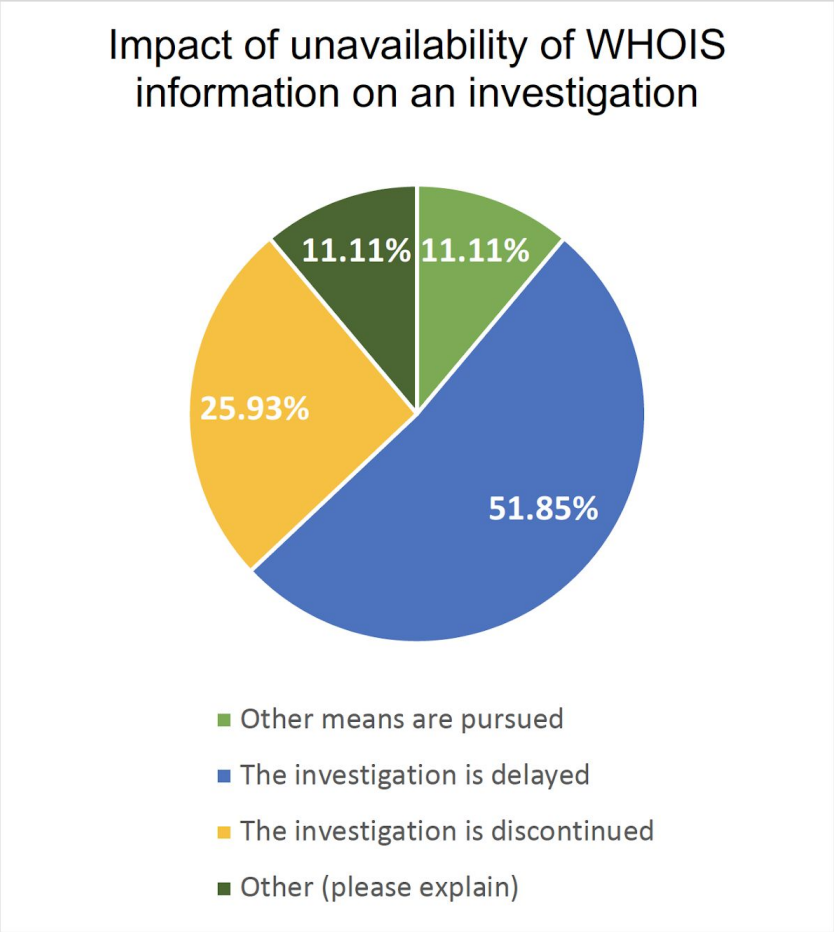


Source: WHOIS-RDS2 Review Team Initial Report Webinar, 17 September 2018

WHOIS/GDPR - Impact on Law Enforcement

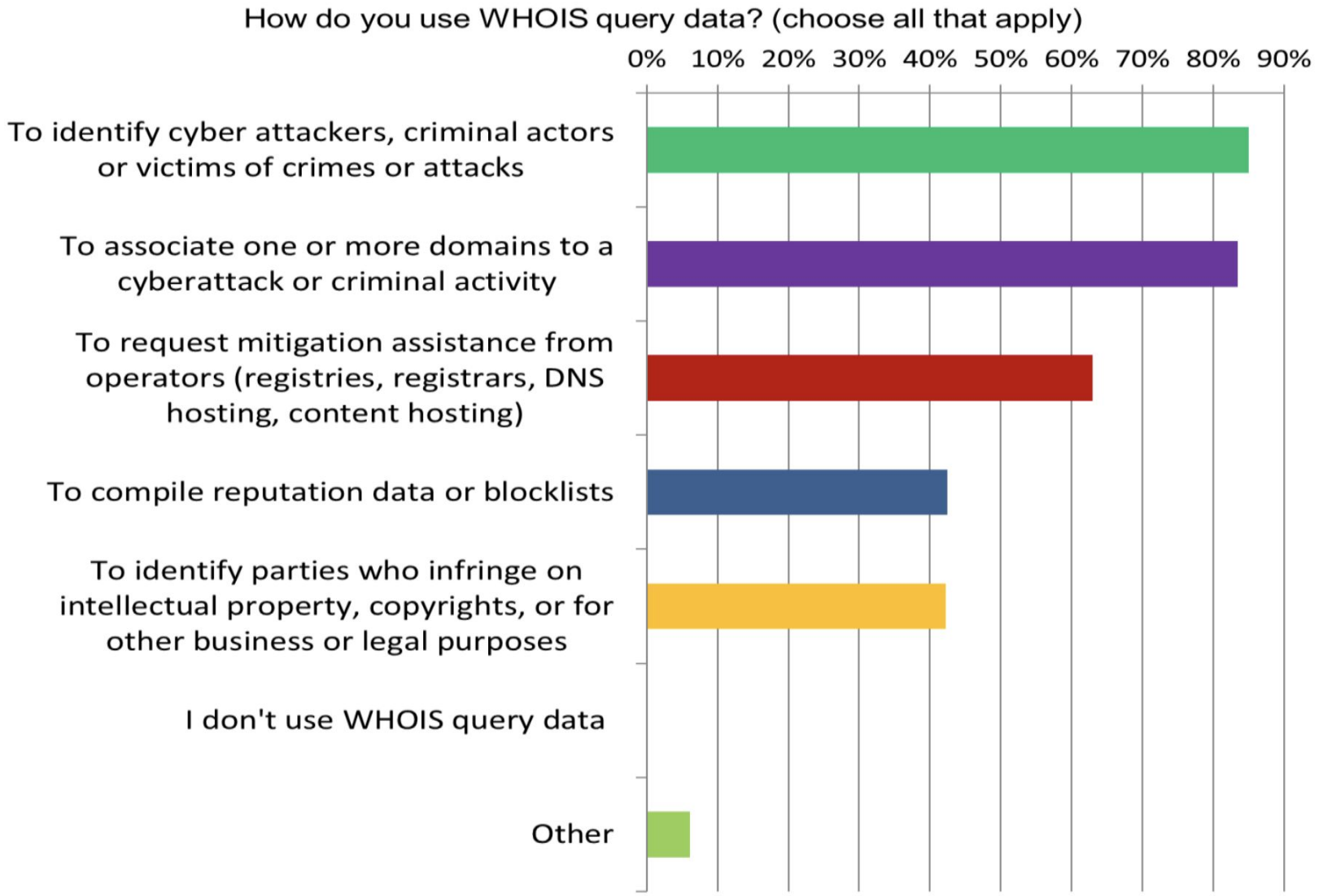
Impact of Unavailability





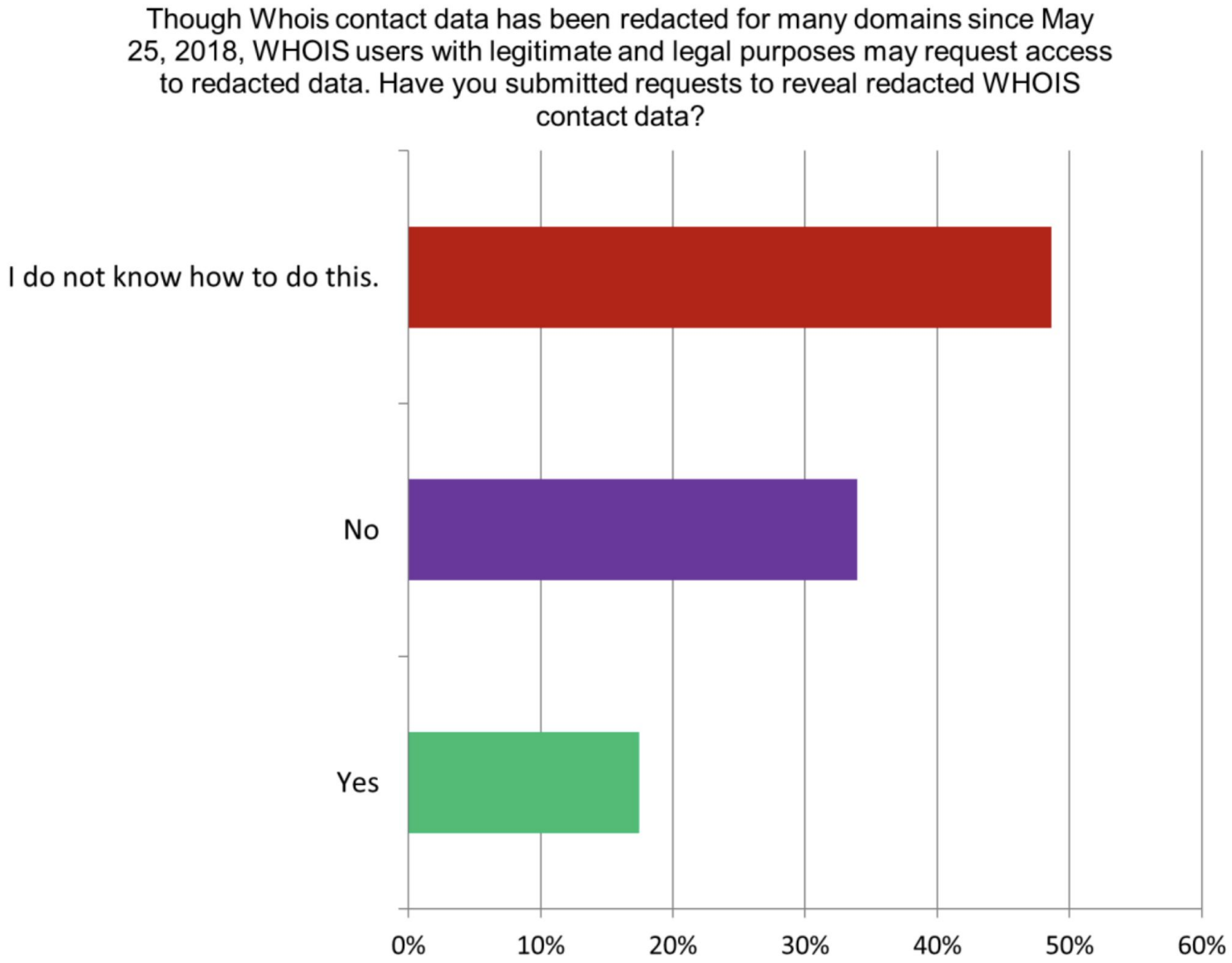
Source: WHOIS-RDS2 Review Team Initial Report Webinar, 17 September 2018

WHOIS/GDPR - Impact on Cybersecurity



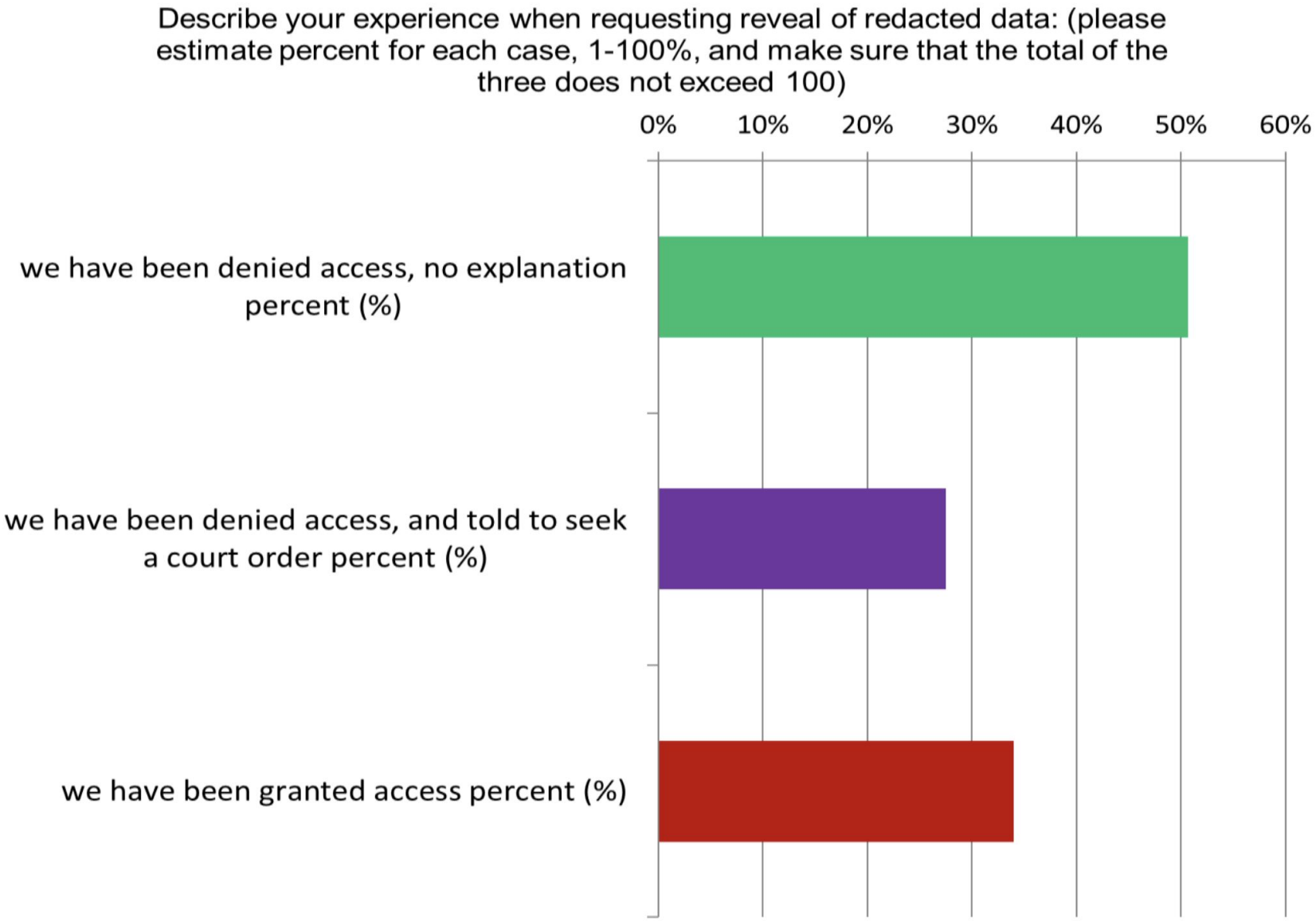
Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Cybersecurity



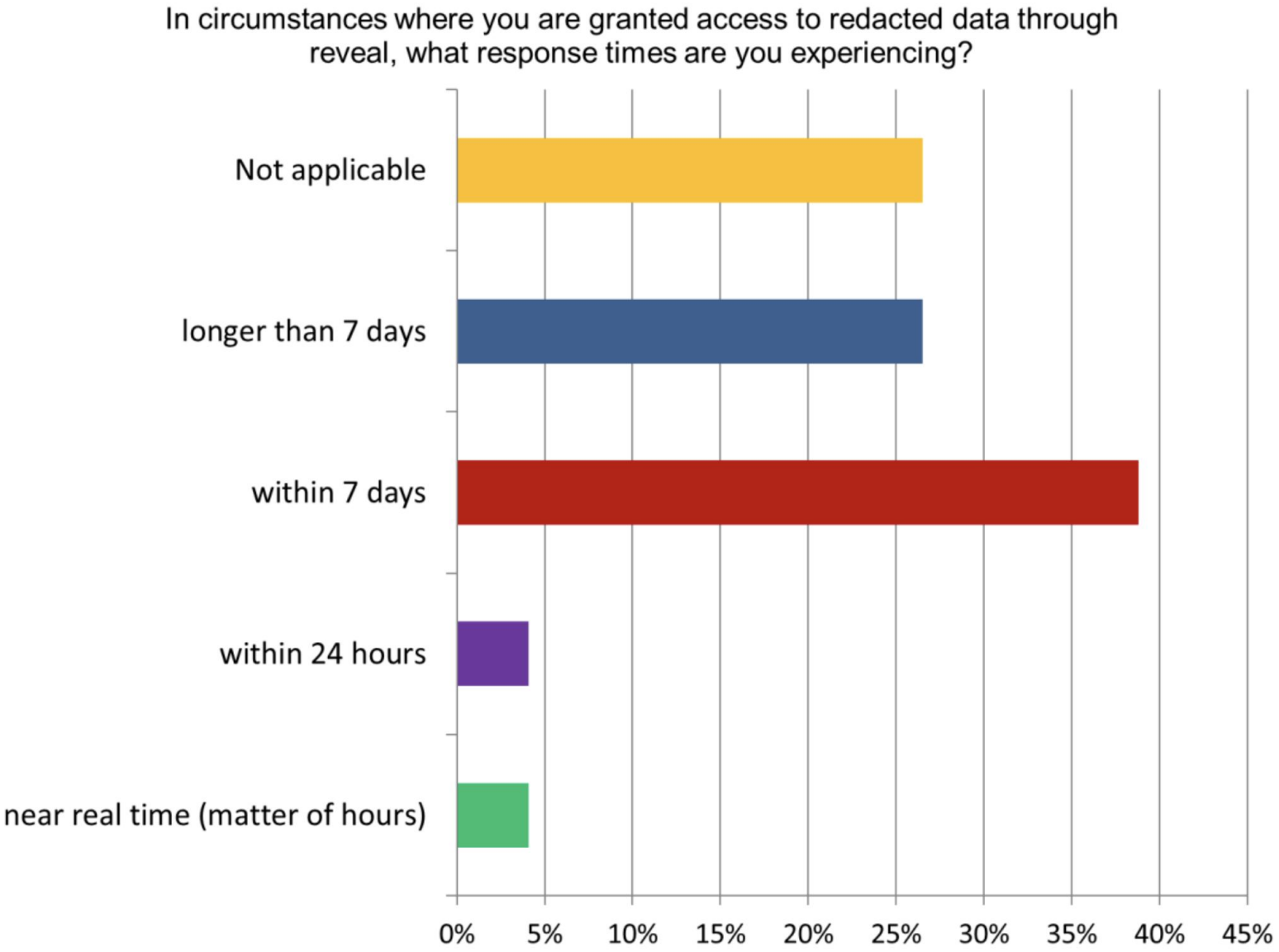
Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Cybersecurity



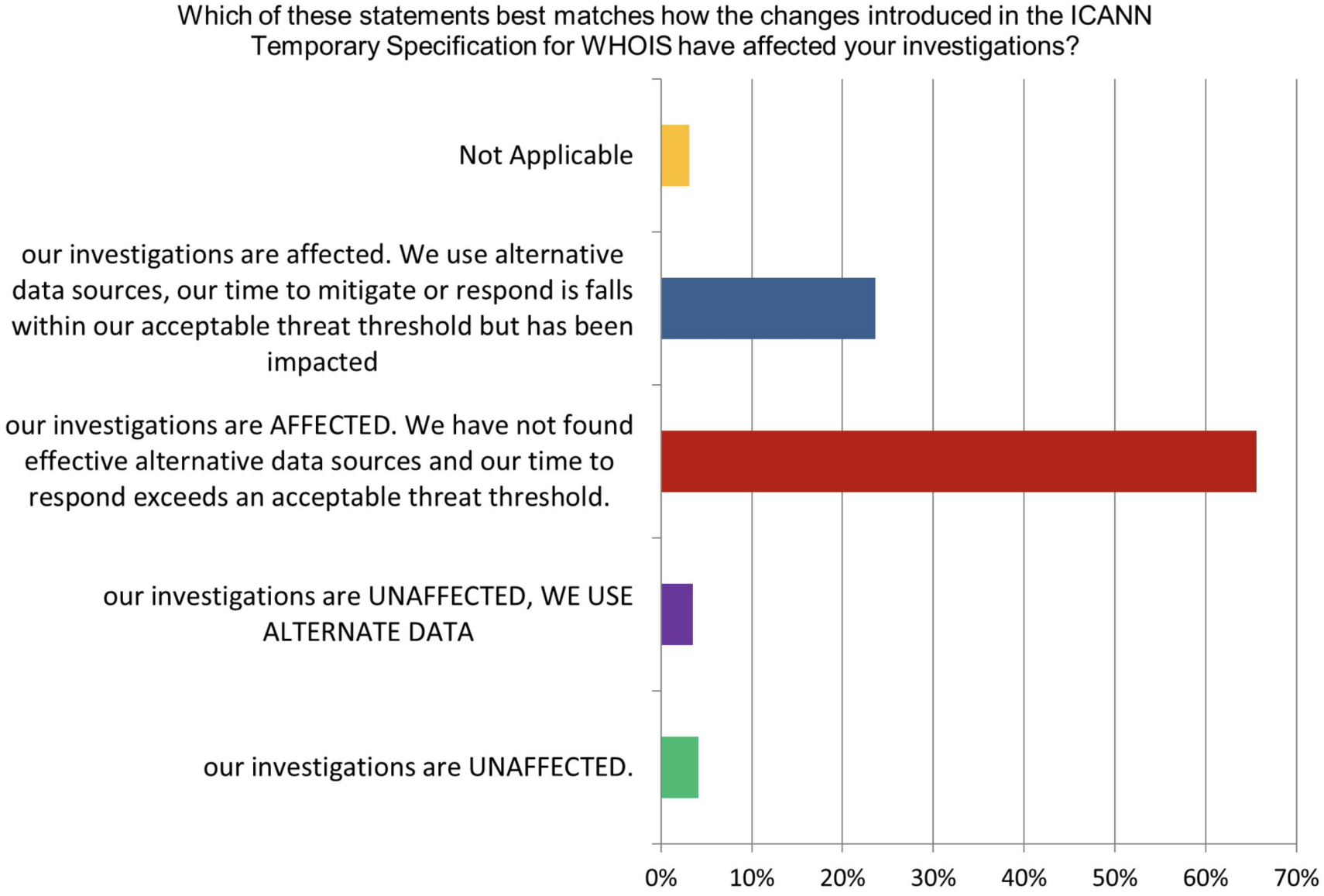
Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Cybersecurity



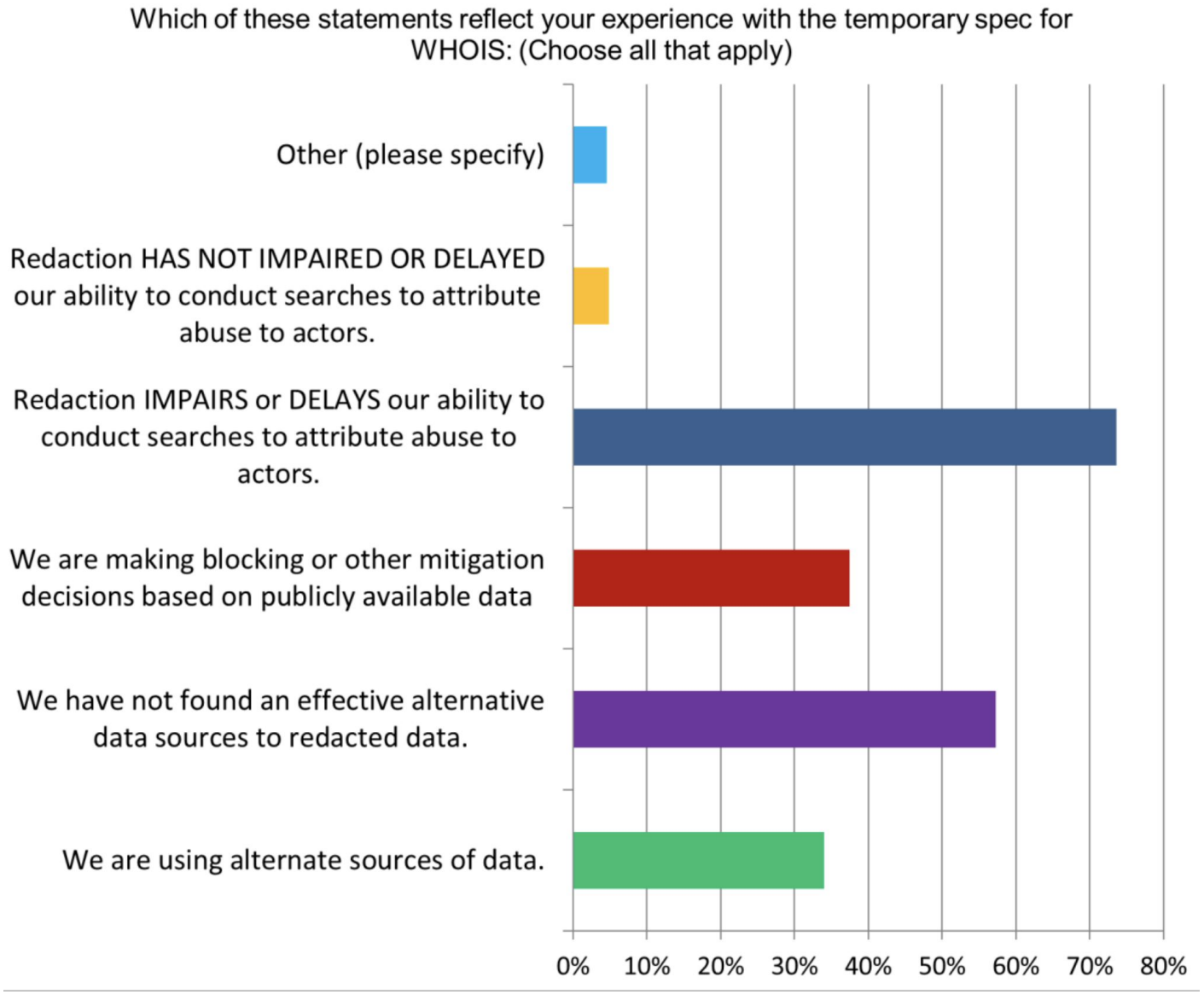
Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Cybersecurity



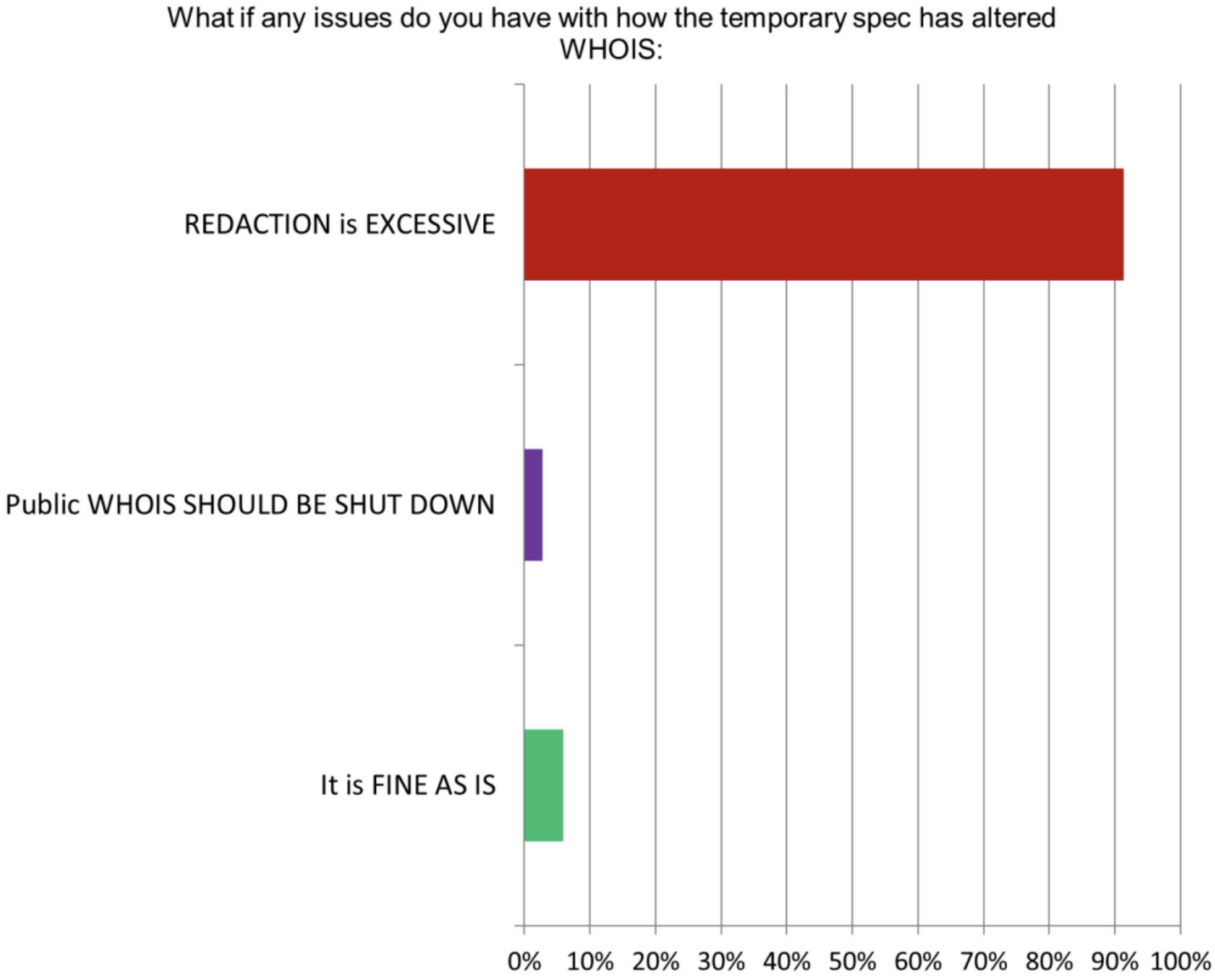
Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Cybersecurity



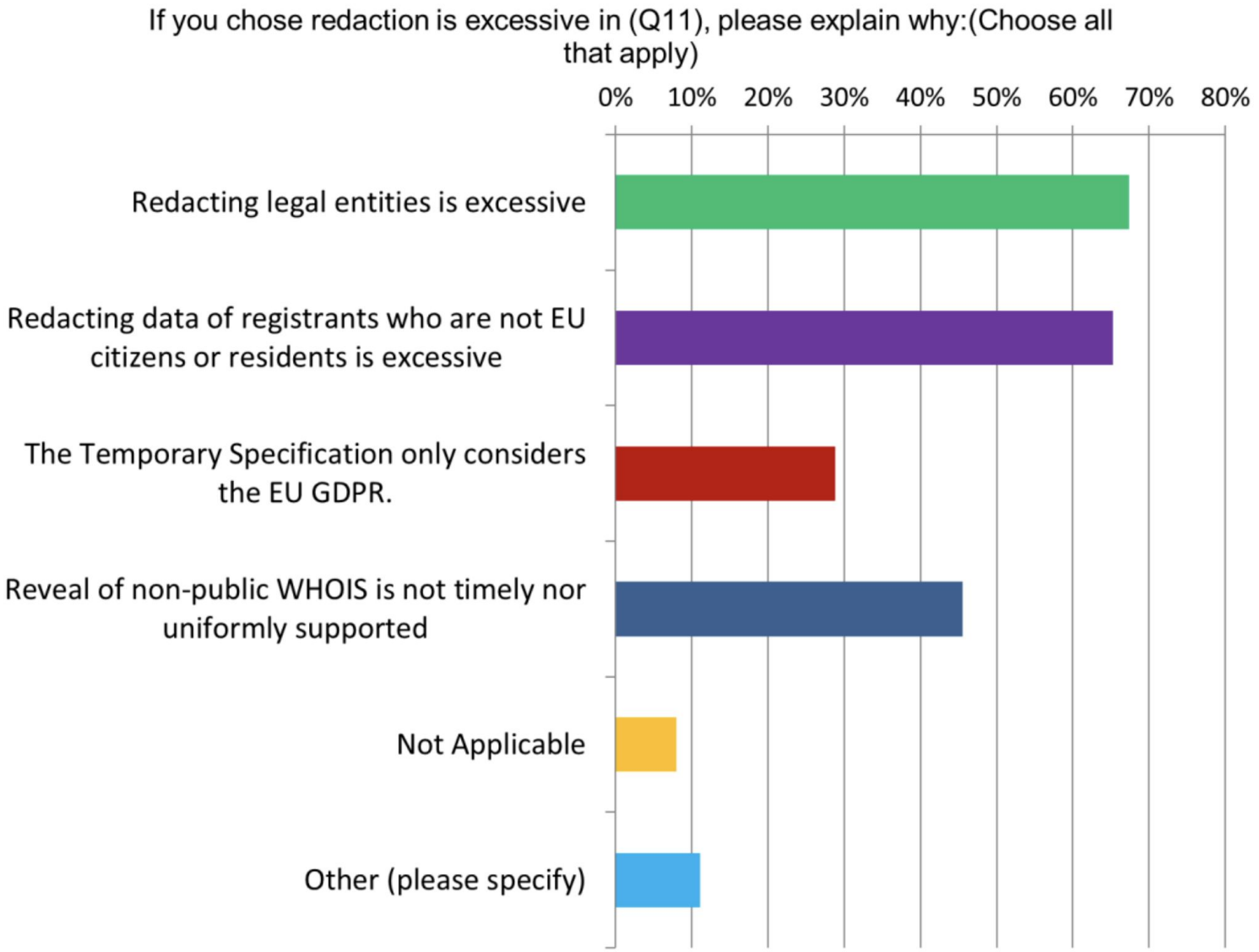
Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Cybersecurity



Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Cybersecurity



Source: ICANN GDPR and WHOIS Users Survey, APWG & MAAWG, 18 October 2018

WHOIS/GDPR - Impact on Law Enforcement

- Requests for non public data to registrars have inconsistent, unpredictable results
- Temporary specification is too vague regarding access to non public data
- Some registrars are not providing reasonable access by systematically requiring court orders
- Investigations take longer; victims at risk longer
- Not seeing the full impact on investigations yet:
  - LEA still have access to pre 25 May 2018 data
  - Nevertheless, ability to attribute crime is degrading

WHOIS/GDPR - Needs of Law Enforcement

- Immediate access to non public data via central portal
- Reverse Lookup (Searchability of Whois)
- Historical Whois (Requires longer data retention)
- Single and multiple query capabilities
- Cybersecurity researchers' access to non public data (including reverse lookup)

Agenda

1. Introduction and Review of PSWG Activities

2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement

3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)